## REMARKS

Claims 1-58 are pending in the present application. In a January 26, 2007, Office Action (herein "Office Action"), Claims 1, 2, 14, 18-22, 31-36, 42, 43, 45-50, 56-58 were rejected under 35 U.S.C. § 103(a) as being obvious in view of by U.S. Patent No. 6,023,223 issued to Baxter et al. (herein "Baxter") and in further view of a publication entitled "Focus on OpenView: A Guide to Hewlett-Packard's Network and Systems Management Platforms" (hereinafter "OpenView"). Claims 3-7, 9-13, 15-17, 24, 25, 37-41, and 51-55 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Baxter in view of U.S. Patent No. 6,714,977 to Fowler (herein "Fowler"). The Office Action rejected Claims 8, 23, 26, and 44 under 35 U.S.C. § 103 as being unpatentable over Baxter, Fowler, and in further view of in view of U.S. Patent No. 6,429,893 to Xin (herein "Xin"). The Office Action rejected Claims 28-30 under 35 U.S.C. § 103 as being unpatentable over Baxter, Fowler, and further in view of U.S. Patent No. 6,219,439 to Burger (herein "Burger"). Applicants respectfully submit that the rejected claims of the present application are non-obvious over the cited references, alone or in combination, because the cited references fail to teach or suggest an integrated information system in which security information is continuously transmitted to a central location, among other claim elements.

Pursuant to 37 C.F.R. § 1.111, and for the reasons set forth below, applicants respectfully request reconsideration and allowance of the pending claims. Prior to presenting the reasons why applicants believe that the pending claims are in condition for allowance, a brief summary of the present invention, as well as the cited references are presented. However, it should be appreciated that the following summaries are presented solely to assist the Examiner in recognizing the differences between the pending claims and the cited references, and should not be construed as limiting upon the present invention.



LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Summary of the Present Application

The present application is generally directed toward a system and method of implementing a configurable security monitoring system for a plurality of remote monitoring sites. In accordance with an illustrative embodiment, a method is provided that obtains monitoring device data from the at least one monitoring device and one or more rules. The one or more rules establish a threshold for the monitoring device data based on input received from the monitoring device. The input is processed according to the monitoring rules to determine whether a rule violation has occurred. When a rule violation is identified, an authorized user may be notified of the violation.

Summary of Baxter et al. (U.S. Patent No. 6,023,223)

Baxter is purportedly directed at a system and method for early warning detection and notification of environmental conditions. In this regard, Baxter uses a plurality of remotely located environmental sensors having a communication uplink to one or more Earth-orbiting satellites or other wireless transmission means. The environmental sensors periodically upload environmental condition data to a satellite. Then, the satellite downloads the condition data to the database server where an interface provides access to the condition data through a network such as the Internet. The environmental conditions monitored by the system in Baxter include hydrocarbon concentrations, water temperature, wind speed, plate tectonics, atmospheric pressure, toxin concentrations, and the like. Additional applications may include tracking of animal migrations and densities, deforestation, polar ice cap activity, red tide, and other geological, biological, atmospheric, and oceanic conditions.

Summary of Fowler et al. (U.S. Patent No. 6,714,977)

Fowler is purportedly directed toward a system and method for monitoring an enclosed space over a communication network. Generally described, Fowler teaches the utilization of



LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

various low cost, independent monitoring components (e.g., "bots"), that monitor and report various conditions associated with a monitored space. Each bot is specifically configured to monitor specific parameters, such as a climate bot, a video climate bot, a net bot, etc. In turn, each bot processes raw monitored data and provides processed data to a user over a communication network.

Claims 1, 2, 14, 18-22, 31-36, 42-43, 45-50, and 56-58

The Office Action rejected Claims 1, 2, 14, 18-22, 31-36, 42-43, 45-50, and 56-58 under 35 U.S.C. § 103 as being obvious in view of Baxter and in further view of OpenView. Applicants respectfully disagree. As described in more detail below, the cited reference fails to disclose or suggest certain elements of the independent and dependent claims and are non-obvious over the cited references.

Claims 1, 34, and 48

For purposes of this discussion, independent Claims 1, 34, and 48 of the present application will be discussed together because the same distinguishing elements over in Baxter and the other cited references are recited in each of these claims. In this regard, Claim 1 recites the following:

> In an integrated information system including a central server in communication with two or more geographically distinct sites, a method for processing monitoring device data, the method comprising:
>
> obtaining monitoring device data from the two or more geographically distinct sites, wherein the monitoring device data corresponds to two monitoring devices with at least one monitoring device at each geographically distinct site wherein the monitoring device data is obtained continuously;
>
> obtaining one or more monitoring rules corresponding to the at least one monitoring device, wherein the one or more rules establish the thresholds of monitoring device data that define a rule violation;



LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

processing the monitoring device data at the central server according to the monitoring rules to determine whether a rule violation occurred wherein a rule violation identifies a combination of thresholds for each of the two monitoring devices;

wherein processing the monitoring device data according to the rules includes determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred; and

generating an output corresponding to the processing of the monitoring device data, wherein the output indicates whether a rule violation occurred.

Similarly, Claim 34 recites the following:

A system for implementing an integrated information system, the system comprising:

one or more monitoring devices corresponding to two or more geographically distinct sites organized according to geographic criteria and operable to continuously transmit monitoring device data;

a central processing server, the central processing server operable to continuously obtain the monitoring device data from at least one monitoring device at each of the two or more geographically distinct sites;

wherein the central processing server processes the monitoring device data according to one or more monitoring device rules corresponding to the one or more monitoring devices organized according to geographic criteria, wherein the central processing server generates an output corresponding to the processing, wherein the output reflects the results of processing the monitoring device data according to the rules;

wherein the processing of monitoring device data performed by the central processing server includes determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred; and

wherein the monitoring device rules identify a combination of thresholds for the monitoring device data that define a rule violation.

Similarly, Claim 48 recites the following:

A system for implementing an integrated information system, the system comprising:



LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

one or more monitoring devices operable to continuously transmit monitoring device data from two or more geographically distinct sites organized according to geographic criteria; and

central processing means for continuously obtaining the monitoring device data from the one or more monitoring devices, processing the monitoring device data according to one or more monitoring device rules corresponding to the one or more monitoring devices organized according to geographic criteria and generating outputs corresponding to the processing, wherein-the output reflects the results of processing the monitoring device data according to the rules;

wherein the processing of monitoring device data performed by the processing means includes determining whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premises has occurred; and

wherein the monitoring device rules identify a combination of thresholds

for the monitoring device data that define a rule violation.Each of the

independent Claims 1, 34, and 48 recites processing the monitoring device data according to rules for the purpose of determining "whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premise has occurred." In contrast to the claims of the present invention, Baxter is directed to an Internet-based global network for retrieving, storing, and displaying real time environmental data. In this regard, Baxter describes a computer system that includes remotely located environmental sensors having a communications uplink to a communication relay, a downlink interface from the satellite to a database server having one or more data tables holding environmental data. Applicants respectfully submit that applying a set of rules to determine whether an unauthorized access to a premise is occurring is fundamentally different than collecting and evaluating data obtained using environmental sensors to identify environmental emergencies. For example, aspects of the present invention may be used to determine whether a person is burglarizing a premises. By contrast, an example use of Baxter is determining whether received environmental data indicates that an earthquake has occurred. Applying a set of rules to received data that is used to

determine whether a burglary is occurring is fundamentally different than measuring environmental conditions to determine whether a natural disaster is occurring. More specific to the recitations in independent Claims 1, 34, and 48, Baxter simply does not teach or suggest determining "whether the monitoring device data exceeds thresholds of security information indicative of whether an unauthorized access to a premise has occurred." Simply stated, the "tangible result" of the present invention of determining whether an "unauthorized access" of the premises has occurred, is not equivalent to the tangible result of Baxter, namely, to determine whether an environmental emergency has occurred.

The cited and applied references also fail to teach or suggest a system in which security "data is obtained continuously" from geographically distinct sites for determining whether an unauthorized access to a premise has occurred. The Office Action asserts that Baxter teaches an integrated information system wherein the data is obtained continuously and cites column 6, lines 33-48, and column 8, lines 29-35, of Baxter in support of that proposition. The cited portions of Baxter recite obtaining "streaming environmental data from sensors 15a-c." From the use of term "streaming environmental data," the Office Action "implies" that Baxter continually receives security data from the remote location. However, this implication misconstrues the teachings of Baxter. In this regard, Baxter explicitly states that the remote "sensors *periodically* upload environmental condition data to the satellite, the satellite downloads the condition data to the database server, the communication interface provides access to the condition data through the Internet." (Emphasis added.) Baxter at column 3, lines 14-19. Moreover, the Baxter reference explicitly indicates throughout the disclosure that data is periodically obtained and not obtained continuously as implied in the Office Action, stating:

> Thus, at periodic intervals, new data gathered by the satellites is emailed to the end-user for analysis. This method permits the end-user to create a personal archive of historical data for a particular query. (Baxter at column 5, lines 1-4.)

> Remotely located oil detection buoys in the Gulf of Mexico periodically relay hydrocarbon concentrations to orbiting satellites which then transmit the data to the web server. (Baxter at column 5, lines 16-20.)
>
> Remotely located sensors 15a-c may be pre-configured to periodically upload diagnostic information through the communications uplink. (Baxter at column 7, lines 44-48.)
>
> A communications interface between said database server and a data network wherein said sensors periodically upload environmental condition data. (Baxter at column 9, lines 11-15).

While periodically uploading environmental condition data to a satellite may have benefits when environmental conditions are being monitored, the system disclosed in Baxter could not be applied to obtaining security data. More specifically, by periodically uploading data, the Baxter system does not satisfy the time sensitive requirements of a security monitoring system. In contrast to the system disclosed in Baxter, Claims 1, 34, and 48 of the present invention recite obtaining monitoring device data continuously. For example, the monitoring device data may be obtained continuously when a central server polls the monitoring device data from a remotely located monitoring device.

The Office Action acknowledges that Baxter does not define rules in which thresholds of monitoring device data from two monitoring devices are used to establish a rule violation. However, the Office Action asserts that the combined teachings of Baxter with OpenView render this claim element obvious. However, OpenView merely describes utilizing Boolean expressions. In contrast to the present invention, the cited references do not teach, either alone or in combination, a software system for identifying a combination of thresholds for determining whether an authorized access to a premises has occurred. At most, the combined teachings of Baxter and OpenView teach how to use Boolean expressions in analyzing obtained environmental data. However, applicants respectfully submit that using Boolean expressions in order to process environmental data is not equivalent to defining a set of rules "in which

thresholds of monitoring device data from two monitoring devices are used to establish a rule violation."

As described above, Baxter fails to teach or suggest an integrated information system in which security data to determine whether an unauthorized access to a premises has occurred is obtained continuously, as alleged in the Office Action. Moreover, the combined teachings of Baxter and OpenView do not teach or suggest obtaining one or more monitoring rules wherein a rule violation identifies a combination of thresholds for the monitoring devices. Since Baxter and the other cited references fail to teach each element recited in Claims 1, 34, and 38, applicants respectfully request a withdrawal of the 35 U.S.C. § 103 rejection of these claims.

Claims 14, 18-22, 31-33, 35-36, 42-43, 45-47, 49-50, 56-58

Claims 14, 18-22, 31-33, 35-36, 42-43, 45-47, 49-50, 56-58 depend on independent Claim 1, 34, and 48, respectively. As discussed above, Baxter fails to teach or suggest an integrated information system in which security data to determine whether an unauthorized access has occurred is obtained continuously. Moreover, the combined teachings of Baxter and OpenView do not teach or suggest obtaining one or more monitoring rules wherein a rule violation identifies a combination of thresholds for the monitoring devices. Accordingly, for the above-mentioned reasons, Claims 14, 18-22, 31-33, 35-36, 42-43, 45-47, 49-50, and 56-58 are also allowable. Additionally, Claims 2, 14, 18-22, 31-33, 35-36, 42-43, 45-47, 49-50, and 56-58 are non-obvious over the combined teachings of Baxter and OpenView, as alleged in the Office Action, for additional reasons discussed below.

Claim 14 adds the additional limitation of generating a communication to one or more designated users, wherein generating the communication includes identifying a hierarchy that prioritizes the communication to the one or more designated users. The Office Action asserts that Baxter teaches generating a communication to one or more designated users. Applicants



LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

agree that the Baxter system is configured to communicate with designated users when an abnormal condition is identified, such as abnormal environmental conditions. In this instance, a communication that is widely distributed may be created and transmitted. However, the Baxter system does not include identifying a hierarchy that prioritizes the communication to the one or more designated users, as disclosed in the present application. In this regard, aspects of the present invention are able to distribute information to the appropriate user. If the appropriate user is not readily available by telephone, then the user may be contacted using other communication means, such as fax, pager, and the like. Accordingly, Baxter fails to teach or suggest the additional element recited in Claim 14. Thus, applicants assert that this claim is also allowable for this additional reason.

Claim 19 has the additional recitation of "generating an output corresponding to the processing of the monitoring device data includes initiating an action at a geographically distinct site where the monitoring data was obtained." As mentioned previously, the Baxter system is directed at collecting environmental data from sensors that may be remotely located. In contrast, aspects of the present invention are directed at securing premises from unauthorized access. In this regard, processing performed by the present invention may determine that an unauthorized access has occurred in response to a rule violation. In this instance, additional actions that occur at a geographic site where the monitoring data was obtained may be performed. For example, aspects of the present invention may cause an audible alarm to be sounded, thereby giving audible notice that an unauthorized access is occurring. Applicants respectfully assert that Baxter in no way teaches initiating an action at a geographic site where monitoring device data was obtained. Accordingly, applicants further assert that Baxter fails to teach or suggest the additional limitation of Claim 19.

Claims 3-7, 9-13, 15-17, 24, 25, 37-41, and 51-55

The Office Action rejected Claims 3-7, 9-13, 15-17, 24, 25, 37-41, and 51-55 under 35 U.S.C. § 103 as being unpatentable over Baxter in view of Fowler. The Office Action asserts that Baxter and Fowler disclose each of the elements of applicants' claims and that it would have been obvious to a person of ordinary skill in the art to combine the teachings of the cited references at the time this invention was made. As described in more detail below, the cited references fail to disclose or suggest elements of these dependent claims. Moreover, applicants submit that it would not have been obvious to combine the teachings of the cited references at the time the invention was made.

Claims 3-7, 9-13, 15-17, 24, and 25 depend from independent Claim 1. Similarly, Claims 37-41 and 51-55 depend from independent Claims 34 and 48, respectively. As discussed above, Baxter fails to teach or suggest an integrated information system in which monitoring device data is obtained continuously. Accordingly, for the above-mentioned reasons, Claims 3-7, 9-13, 15-17, 24, 25, 37-41, and 51-55 are allowable over Baxter alone, or in combination with Fowler. Additionally, Claims 3-7, 9-13, 15-17, 24, 25, 37-41, and 51-55 further add to the non-obviousness of applicants' invention, some of the details of which are discussed below.

Claim 3, 37, and 51 add the additional limitation of "wherein the one or more monitoring devices are characterized as asset data, resource data, or event data, wherein asset data includes data from an identifiable object that is not capable of independent action, wherein resource data includes data from an object capable of independent action, and wherein event data includes data from a device having a defined state." The Office Action asserts that Baxter teaches obtaining asset data and resource data. Office Action at page 6. Then, the Office Action acknowledges that Baxter does not disclose obtaining sensor data from a device having a defined state.

However, the Office Action asserts that Fowler discloses another integrated information system for processing monitoring device data which discloses obtaining event data from a device having a defined state. Applicants respectfully submit that the Office Action is reading into the disclosure of Baxter and Fowler the limitation of characterizing the monitoring device data as asset data or resource data. While the Baxter system may characterize data in certain ways by determining whether the data relates to temperature levels, hydrocarbon levels, and the like, applicants are unable to find any characterization performed by Baxter that differentiates the data based on the type of monitoring device that the data was collected. Accordingly, the cited references fail to teach or suggest the additional elements recited in Claims 3, 37, and 51. Thus, applicants assert that these claims are also allowable for these additional reasons.

Claim 7 adds the additional limitation of "wherein the device rules establish a state threshold for a rule violation and wherein processing the monitoring device data according to the device rules includes determining whether the monitoring device data indicates a particular state." The Office Action asserts that Fowler discloses that the device rules establish a state threshold for a rule violation and determining whether the monitoring device data indicates a particular state. In support of that proposition, the Office Action refers to Figure 17 of Fowler that illustrates the triggering of a smoke alarm. Applicants respectfully submit that rules which establish a state threshold for a rule violation is not equivalent to using an off-the-shelf smoke alarm to indicate a particular state. Accordingly, the cited references fail to teach or suggest the additional element recited in Claim 7.

In regard to Claims 15-17, the Office Action took "Official Notice" that both the concept and advantages of maintaining a schedule of preferred notification methods based on a time of day and preferred notification methods for each designated user is well known and expected in the art. Applicants respectfully disagree. As distinctly claimed in Claims 15-17, "a schedule of



LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

preferred notification methods" is used to determine how an authorized user will be notified of a rule violation. While Fowler does disclose notifying an authorized user, Fowler does not disclose a method for selecting the appropriate notification method that depends on a variable such as the time of day. The Office Action incorrectly equates contacting an authorized user with processing performed to identify a schedule of preferred notification methods. Then, the Office Action inappropriately takes Official Notice that the concept and advantages of providing a schedule of preferred notification methods is well known and expected in the art.

Claims 8, 23, 26, and 44

The Office Action rejected Claims 8, 23, 26, and 44 under 35 U.S.C. § 103 as being unpatentable over Baxter, Fowler, and in further view of in view of U.S. Patent No. 6,429,893 to Xin (herein "Xin"). The Office Action asserts that Baxter, Fowler, and Xin disclose each of the elements of applicants' claims and that it would have been obvious to a person of ordinary skill in the art to combine the teachings of the cited references at the time this invention was made. Applicants respectfully disagree. As described in more detail below, the cited references fail to disclose or suggest elements of these dependent claims. Moreover, applicants submit that it would not have been obvious to combine the teachings of the cited references at the time the invention was made.

Claim 8, adds to the non-obviousness of applicants invention the limitation of "wherein the monitoring device data is motion detection data and wherein the device rule threshold is the detection of motion." The Office Action states that "it is an inherent feature to any motion detector that there must be a lower limit threshold to flag an alert (such as a person walking by, not a piece of paper blowing in the wind)." Office Action at page 12. However, the limitation as recited in Claim 8 do not refer to the inherent abilities of a motion detector. Instead, the limitation recited in Claim 8 refers to processing the data produced from the motion detector in

accordance with a rule. For example, a rule may be established in which a rule violation does not occur until a motion detector detects motion for a specified period of time (e.g., 10 seconds). This ability as reflected in the additional limitation recited in Claim 8 does not appear in any of the cited references.

Claims 27-30

The Office Action rejected Claims 27-30 under 35 U.S.C. § 103 as being unpatentable over Baxter, Fowler, Xin, and further in view of U.S. Patent No. 6,219,439 to Burger (herein "Burger"). Claims 27-30 depend from independent Claim 1. As discussed above, Baxter fails to teach or suggest obtaining monitoring device data continuously. Accordingly, for the above-mentioned reasons, Claims 27-30 are allowable over Baxter alone, or in combination with Fowler, Xin, and Burger. Additionally, Claims 27-30 further add to the non-obviousness of applicants' invention, some of the details of which are discussed below.

Claims 28 adds to the nonobviousness of applicants invention the limitation of using the monitoring device to identify the location of the individuals within the premises. Applicants are unable to find any teaching in the cited references that describe identifying the location of an individual within a premise. Applicants agree that Burger teaches using a "smart card" to verify an individual's identity. However, Burger does not teach identifying the location of an individual within a premise. The Office Action incorrectly equates verifying an individual identity with determining the location of a user within a premise.

CONCLUSION

In view of the amendments and remarks above, applicants respectfully submit that the pending claims are in condition for allowance. Reconsideration and reexamination of the application, as amended, and allowance of the claims at an early date are solicited. If the

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Examiner has any questions or comments concerning the foregoing response, the Examiner is invited to contact the applicants' undersigned attorney at the number below.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS[PLLC]

Clint J. Feekes
Registration No. 51,670
Direct Dial No. 206.695.1633

CJF:jlg



LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100